UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

"CAMPOS CUADRATICOS"

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A

JOSE FERNANDO GARCIA GARCIA

MEXICO, D.F. 1984

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

CONTENIDO

INTRODUCCION

El propósito de esta tesis, es exponer de manera clara la Teoría de las Extensiones Algebraicas Cuadráticas y la Ecuación de Pell. Estos temas son fundamentales en la Teoría de los Números y deberían ser ampliamente conocidos, ya que son un ejemplo de la Teoría de Números Algebraicos.

Esta es una área de la Teoría de los Números en la que hay muchos problemas sin resolver pero que requieren tecnicas muy avanzadas.

§.1. CAMPOS CUADRATICOS

Denotaremos con $\mathbb{Z}=\{..,-2,-1,0,1,2,..\}$ el conjunto de los números enteros racionales y con $\mathbb{Q}=\{a/b \,/\, a\in\mathbb{Z}, b\in\mathbb{Z} \text{ y } b\neq 0\}$ el conjunto de los números racionales.

Def. 1.1. Un Campo es un conjunto F y dos operaciones, adición y multiplicación, que satisfacen las siguientes propiedades:

i) F es un grupo abeliano bajo la adición.

ii) $F-\{0\}$ es un grupo abeliano bajo la multiplicación.

iii) Para todo a, b y c en F, $a(b+c)=ab+ac$.

$\mathbb{Q}$ es un campo.

Def. 1.2. Sea $\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d} \,/\, a \text{ y } b \text{ están en } \mathbb{Q}$ con d en $\mathbb{Q}$ al cual no es el cuadrado de un número racional.

Si $d>0$, entonces $\mathbb{Q}(\sqrt{d})$ es un Campo Cuadrático Real.
Si $d<0$, entonces $\mathbb{Q}(\sqrt{d})$ es un Campo Cuadrático Complejo o Campo Cuadrático Imaginario.

Dado que cualquier número racional a puede estar escrito en la forma $a+0\cdot\sqrt{d}$, $\mathbb{Q}(\sqrt{d}) \supset \mathbb{Q}$.

Si d fuera al cuadrado de un número racional, entonces $a+b\sqrt{d}$ es racional con a y b racionales y así $\mathbb{Q}(\sqrt{d})$ sería $\mathbb{Q}$. Es por esta razón que la definición de campo cuadrático excluye la posibilidad de que d sea al cuadrado de un número racional.

A lo largo del tema las letras del alfabeto a, b, c ... x, y, z. estarán representando elementos de $\mathbb{Z}$ o de $\mathbb{Q}$, con la posible excepción de x, y y z. Las letras del alfabeto griego $\alpha, \beta, \gamma, \ldots$ representarán elementos de $\mathbb{Q}(\sqrt{d})$.

La letra d será un racional con la condición de que $\sqrt{d}$ no sea racional.

Lema 1.3. Si α es irracional y a y b son racionales con $b \neq 0$, entonces $a+b\alpha$ es irracional.

Dem: Sea $x = a+b\alpha$

entonces $b\alpha = x-a$

$$\alpha = \frac{x-a}{b}.$$

Por lo tanto, si x es racional, entonces x-a y x-a/b son racionales. Pero α es irracional, y así que x debe de ser irracional.

Lema 1.4. Supóngase que a y b están en $\mathbb{Q}$ α irracional. Si $a+b\alpha$ es racional, entonces $b=0$.
Si $a+b\alpha = 0$, entonces $a=b=0$.

Dem: Si $b \neq 0$, entonces por el Lema 1.3. $a+b\alpha$ podría ser irracional por lo tanto $b=0$.
Dado que el 0 es racional, $a+b\alpha=0$ implica que $b=0$, por lo tanto

$$a = a+0\cdot\alpha = a+b\alpha = 0.$$

TEO. 1.5. (i) $a+b\sqrt{d}=0$ si y sólo si $a=b=0$.

(ii) $a+b\sqrt{d}=c+e\sqrt{d}$ si y sólo si $a=c$ y $b=e$.

Dem: (i) se cumple por el Lema 1.4.

(ii) Si $a+b\sqrt{d}=c+e\sqrt{d}$,

entonces $(a-c)+(b-e)\sqrt{d}=0$.

De aquí por el Lema 1.4.

$$a-c=0 \quad y \quad b-e=0$$

y se sigue por tanto

$$a=c \quad y \quad b=e.$$

TEO. 1.6. Si α y β son elementos de $\mathbb{Q}(\sqrt{d})$ entonces $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ y para $\beta\neq 0$, α/β están en $\mathbb{Q}(\sqrt{d})$.

Dem: Sean $\alpha=a+b\sqrt{d}$ y $\beta=c+e\sqrt{d}$ elementos de $\mathbb{Q}(\sqrt{d})$ donde $a, b, c, y\ e$ son racionales.

Entonces
$$\alpha+\beta=(a+b\sqrt{d})+(c+e\sqrt{d})$$
$$=(a+c)+(b+e)\sqrt{d}$$
$$\alpha-\beta=(a+b\sqrt{d})-(c+e\sqrt{d})$$
$$=(a-c)+(b-e)\sqrt{d}$$
$$\alpha\beta=(a+b\sqrt{d})(c+e\sqrt{d})$$
$$=(ac+bed)+(ae+bc)\sqrt{d}.$$

Dado que $a+c$, $b+e$, $a-c$, $b-e$, $ac+bed$ y $ae+bc$ están en $\mathbb{Q}$, por tanto

$\alpha+\beta$, $\alpha-\beta$ y $\alpha\beta$ están en $\mathbb{Q}(\sqrt{d})$.

Si $\beta \neq 0$, entonces c y e no son ambos cero y consecuentemente $c-e\sqrt{d} \neq 0$.

Por lo que $c^2-e^2d = (c+e\sqrt{d})(c-e\sqrt{d}) \neq 0$

Así
$$\frac{\alpha}{\beta} = \frac{(a+b\sqrt{d})(c-e\sqrt{d})}{(c+e\sqrt{d})(c-e\sqrt{d})}$$

$$= \left(\frac{ac-bed}{c^2-e^2d}\right) + \left(\frac{bc-ae}{c^2-e^2d}\right)\sqrt{d}.$$

Como $(ac-bed)/(c^2-e^2d)$ y $(bc-ae)/(c^2-e^2d)$ son racionales, α/β está en $\mathbb{Q}(\sqrt{d})$.

TEO. 1.7. $\mathbb{Q}(\sqrt{d})$ es un campo.

En $\mathbb{Q}(\sqrt{d})$ restringimos a la d a no ser el cuadrado de un número racional.

Así que de ahora en adelante d tomará valores enteros racionales que no tengan factores cuadrados mayores que uno, y a este tipo de números los llamaremos "Libres de cuadrados".

Dado que d es diferente de cero y de uno, d no tiene factores cuadrados mayores que uno y por consecuencia d no es un cuadrado perfecto, con lo que $\sqrt{d}$ es irracional.

Los números de la forma $a+b\sqrt{r/s}$ son iguales a los de la forma $a+b\sqrt{rs}$ ya que

$$a+b\sqrt{r/s} = a+b\sqrt{rs/s^2} = a+\frac{b}{s}\sqrt{rs}$$

y así $\mathbb{Q}(\sqrt{r/s}) = \mathbb{Q}(\sqrt{rs})$, es decir, ambos campos consisten de los mismos elementos.

Analogamente $\mathbb{Q}(\sqrt{r^2 s}) = \mathbb{Q}(\sqrt{s})$.

Lema 1.8. Los números de $\mathbb{Q}(\sqrt{d})$ son soluciones de ecuaciones cuadráticas con coeficientes enteros racionales.

Dem: El número $a+b\sqrt{d}$ es raíz de la ecuación

$$X^2 - 2aX + (a^2 - b^2 d) = [X-(a+b\sqrt{d})][X-(a-b\sqrt{d})] = 0,$$

la cual tiene coeficientes racionales, si multiplicamos la ecuación por un común denominador de $(2a)$ y (a^2-b^2d), obtenemos una ecuación cuadrática con coeficientes enteros racionales.

Las dos raíces de esta ecuación, $a+b\sqrt{d}$ y $a-b\sqrt{d}$, se dicen conjugadas una de la otra.

Def. 1.9. Si $\alpha = a+b\sqrt{d}$, entonces definimos el conjugado de α como $\overline{\alpha} = a-b\sqrt{d}$.

Si $d<0$, entonces α y $\overline{\alpha}$ son conjugados como complejos.

TEO. 1.10. Si α y β están en $\mathbb{Q}(\sqrt{d})$, entonces $\overline{(\overline{\alpha})} = \alpha$, $\overline{\alpha+\beta} = \overline{\alpha}+\overline{\beta}$, $\overline{\alpha-\beta} = \overline{\alpha}-\overline{\beta}$, $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$ y si $\beta \neq 0$, entonces $\overline{(\alpha/\beta)} = \overline{\alpha}/\overline{\beta}$. $\alpha = \overline{\alpha}$ si y sólo si α es racional.

Dem: Sean $\alpha = a+b\sqrt{d}$ y $\beta = c+e\sqrt{d}$. Entonces

$$\overline{(\overline{\alpha})} = \overline{(a-b\sqrt{d})} = a+b\sqrt{d} = \alpha.$$

$$\overline{(\alpha+\beta)} = \overline{[(a+c)+(b+e)\sqrt{d}]} = (a+c)-(b+e)\sqrt{d} = \overline{\alpha}+\overline{\beta}.$$

$$\overline{(\alpha-\beta)} = \overline{[(a-c)+(b-e)\sqrt{d}]} = (a-c)-(b-e)\sqrt{d} = \overline{\alpha}-\overline{\beta}.$$

$$\overline{(\alpha\beta)} = \overline{[(ac+bed)+(ae+bc)\sqrt{d}]} = (ac+bed)-(ae+bc)\sqrt{d} = \overline{\alpha}\,\overline{\beta}.$$

Si $\beta \neq 0$, entonces $\overline{\beta} \neq 0$. Así dado que $1/\beta\overline{\beta} = 1/(c^2-e^2d)$ es racional,

$$\overline{\left(\frac{\alpha}{\beta}\right)} = \overline{\left(\frac{\alpha\overline{\beta}}{\beta\overline{\beta}}\right)} = \overline{\left(\frac{1}{\beta\overline{\beta}}\alpha\overline{\beta}\right)} = \left(\frac{1}{\beta\overline{\beta}}\right)\overline{\alpha}\,\overline{\beta} = \frac{1}{\beta\overline{\beta}}\overline{\alpha}\beta = \frac{\overline{\alpha}}{\overline{\beta}}.$$

Si $\alpha = \overline{\alpha}$, entonces $a+b\sqrt{d} = a-b\sqrt{d}$ luego por el TEO. 1.5. se tiene que $b=-b$ y por ésto es que $b=0$ y $\alpha = a$ es racional.

Si $\alpha = a+0\cdot\sqrt{d}$ es racional, entonces

$$\overline{\alpha} = a-0\cdot\sqrt{d} = \alpha.$$

Hemos visto que un número α de $\mathbb{Q}(\sqrt{d})$ satisface una ecuación cuadrática con coeficientes enteros racionales, es decir,

$$ax^2+bx+c=0. \qquad (1)$$

Dado que α satisface esta ecuación y a, b y c son racionales,

$$a(\overline{\alpha})^2+b\overline{\alpha}+c =$$

$$\bar{a}(\overline{\alpha^2}) + \bar{b}\bar{\alpha} + \bar{c} =$$

$$(\overline{a\alpha^2}) + (\overline{b\alpha}) + \bar{c} =$$

$$\overline{(a\alpha^2 + b\alpha + c)} = \bar{0} = 0.$$

En otras palabras, si α es raíz de (1), entonces $\bar{\alpha}$ también lo es.

Si α es irracional, entonces $\alpha \neq \bar{\alpha}$ y de aquí que

$$ax^2 + bx + c = a(x-\alpha)(x-\bar{\alpha}).$$

Sea $\alpha = a' + b'\sqrt{d}$, como α es raíz de (1) se tiene que

$$a(a'+b'\sqrt{d})^2 + b(a'+b'\sqrt{d}) + c = 0$$

y así tenemos

$$aa'^2 + b'da + ba' + c = 0 \qquad (1°)$$

y

$$2aa'b' + bb' = 0 \qquad (2°)$$

Supóngase que $a=1$, en (2°) se tendra la ecuación

$$2a'b' + bb' = 0$$

de donde

$$(2a' + b)\, b' = 0$$

y por lo tanto $b'=0$ o $\boxed{b=-2a'}$ *.

Sustituyamos en (1°) los valores para $a=1$ y de $b=-2a'$, con esto se obtiene la ecuación

$$-a'^2 + b'^2 d + c = 0,$$

por lo que $\boxed{c = a'^2 - b'^2 d}$ **.

Por lo tanto α y $\bar{\alpha}$ satisfacen la ecuación

$$X^2+bX+c=0,$$

con b y c dados por * y **.

Así cuando α es irracional, hay una infinidad de ecuaciones cuadráticas satisfechas por α.

Def. 1.11. Si α es irracional en $\mathbb{Q}(\sqrt{d})$, entonces la ecuación $ax^2+bx+c=0$ es llamada la ecuación mínima satisfecha por α si α satisface la ecuación y a, b y c son enteros racionales, $(a,b,c)=1$, y $a>0$.

Lema 1.12. Si a y n son enteros racionales positivos y $\sqrt[n]{a}$ es racional, entonces $\sqrt[n]{a}$ es entero racional.

Dem: Dado que $\sqrt[n]{a}$ es racional (y positivo), existen enteros racionales r y s tal que $\sqrt[n]{a}=r/s$, aún más $(r,s)=1$.

Mostraremos que $s=1$.

Si $s>1$, entonces existe un primo p tal que $p \mid s$ de donde $p \mid as^n=r^n$ y así $p \mid r$ contradicción ya que $(r,s)=1$.

Por lo tanto $s=1$ y $\sqrt[n]{a}=r$.

TEO. 1.13. La intersección de dos campos cuadráticos diferentes es $\mathbb{Q}$.

Dem: Supóngase que el número irracional

$$\alpha=a+b\sqrt{d}=a_1+b_1\sqrt{d_1}$$

está en $\mathbb{Q}(\sqrt{d})$ y $\mathbb{Q}(\sqrt{d_1})$.

La otra raíz de la ecuación satisfecha por α es

$$\bar{\alpha} = a - b\sqrt{d} = a_1 - b_1\sqrt{d_1},$$

que es la misma en ambos campos.

Dado que $\alpha + \bar{\alpha} = 2a$ y $\alpha + \bar{\alpha} = 2a_1$ se tiene entonces que $a = a_1$.

Por otro lado $\alpha\bar{\alpha} = a^2 - b^2 d$ y $\alpha\bar{\alpha} = a_1^2 - b_1^2 d_1$ de donde

$$a^2 - b^2 d = a_1^2 - b_1^2 d_1$$

$$b^2 d = b_1^2 d_1$$

$$\sqrt{b^2 d} = \sqrt{b_1^2 d_1}$$

$$b\sqrt{d} = b_1\sqrt{d_1}$$

$b \neq 0$, dado que α es irracional,

$$\sqrt{d} = \frac{b_1\sqrt{d_1}}{b}$$

y así

$$\sqrt{dd_1} = \frac{b_1 d_1}{b}.$$

Por el Lema 1.12. $\sqrt{dd_1}$ es entero racional. Pero d y d_1 son libres de cuadrados, el Teorema de factorización única nos asegura que la única manera para que dd_1 pueda ser un cuadrado perfecto es que d y d_1 tengan el mismo signo y estén compuestos de los mismos factores primos.

Así $d = d_1$.

Def. 1.14. Si α está en $\mathbb{Q}(\sqrt{d})$, entonces definimos la Norma de α como $N(\alpha) = \alpha\bar{\alpha}$.

TEO. 1.15. Si a está en $\mathbb{Q}$, entonces $N(a) = a^2$.
Si α está en $\mathbb{Q}(\sqrt{d})$, entonces $N(\alpha)$ es racional.
$N(\alpha) = 0$ si y sólo si $\alpha = 0$.
Si $d < 0$, entonces $N(\alpha) \geq 0$.
Si β también está en $\mathbb{Q}(\sqrt{d})$, entonces

$$N(\alpha\beta) = N(\alpha)\,N(\beta)$$

y, si $\beta \neq 0$,

$$N(\alpha/\beta) = N(\alpha)/N(\beta).$$

Es decir la Norma es un homomorfismo del grupo multiplicativo de $\mathbb{Q}(\sqrt{d})$ en el grupo multiplicativo de $\mathbb{Q}$.

Dem: Si a está en $\mathbb{Q}$, entonces

$$N(a) = a\bar{a} = aa = a^2.$$

Si $\alpha = a + b\sqrt{d}$, entonces

$$N(\alpha) = \alpha\bar{\alpha} = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2 d = a^2 + b^2(-d),$$

el cual es un número racional, y; si $d < 0$, entonces

$$a^2 \geq 0,\ b^2 \geq 0 \text{ y } (-d) \geq 0,$$

y así $N(\alpha) \geq 0$.

$N(\alpha)$ es racional dado que

$$\overline{N(\alpha)} = \overline{(\alpha\bar{\alpha})} = \bar{\alpha}\,\bar{\bar{\alpha}} = \bar{\alpha}\alpha = \alpha\bar{\alpha} = N(\alpha),$$

y por el TEO. 1.10. $N(\alpha)$ es racional.

Obviamente $N(0) = 0$ y, si $\alpha \neq 0$, entonces $\bar{\alpha} \neq 0$ y así $N(\alpha) = \alpha\bar{\alpha} \neq 0$.
Por lo tanto, $N(\alpha) = 0$ si y sólo si $\alpha = 0$.
Ahora,

$$N(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$$

y, si $\beta \neq 0$,

$$N(\alpha/\beta) = (\alpha/\beta)\overline{(\alpha/\beta)} = \alpha/\beta \cdot \bar{\alpha}/\bar{\beta} = N(\alpha)/N(\beta).$$

Def. 1.16. Si α está en $\mathbb{Q}(\sqrt{d})$, entonces definimos la Traza de α como $T(\alpha) = \alpha + \bar{\alpha}$.

TEO. 1.17. Si a está en $\mathbb{Q}$, entonces $T(a) = 2a$. Si α está en $\mathbb{Q}(\sqrt{d})$, entonces $T(\alpha)$ es racional. Si β también está en $\mathbb{Q}(\sqrt{d})$, entonces $T(\alpha+\beta) = T(\alpha) + T(\beta)$.

Es decir la Traza es un homomorfismo del grupo aditivo de $\mathbb{Q}(\sqrt{d})$ en el grupo aditivo de $\mathbb{Q}$.

Dem: Si a está en $\mathbb{Q}$, entonces

$$T(a) = a + \bar{a} = a + a = 2a.$$

$$\overline{T(\alpha)} = \overline{(\alpha + \bar{\alpha})} = \bar{\alpha} + \bar{\bar{\alpha}} = \bar{\alpha} + \alpha = \alpha + \bar{\alpha} = T(\alpha),$$

así por el TEO. 1.10. $T(\alpha)$ es racional.

Si α y β están en $\mathbb{Q}(\sqrt{d})$, entonces

$$T(\alpha+\beta) = (\alpha+\beta) + \overline{(\alpha+\beta)} = (\alpha+\beta) + (\bar{\alpha}+\bar{\beta}) = T(\alpha) + T(\beta).$$

§.2. ENTEROS CUADRATICOS

Def. 2.1. Un número α en $\mathbb{Q}(\sqrt{d})$ es llamado entero cuadrático o entero, si α es racional y está en $\mathbb{Z}$ o si α es irracional y el coeficiente de x^2 en la ecuación mínima satisfecha por α es 1.

TEO. 2.2. Si $d \not\equiv 1 \pmod 4$, entonces los enteros de $\mathbb{Q}(\sqrt{d})$ son los números de la forma $a+b\sqrt{d}$, donde a y b son enteros racionales.
Si $d \equiv 1 \pmod 4$, entonces los enteros de $\mathbb{Q}(\sqrt{d})$ son los números de la forma $(a+b\sqrt{d})/2$, donde a y b son enteros racionales, ambos pares o ambos impares.

Dem: Si $\alpha = a+b\sqrt{d}$, donde a y b son racionales, entonces α es racional si y sólo si $b=0$. Así α es entero racional si y sólo si a está en $\mathbb{Z}$ y $b=0$ y entonces está en la forma

$$\alpha = a+b\sqrt{d} \qquad (a \text{ y } b \text{ en } \mathbb{Z})$$

$$= (2a+2b\sqrt{d})/2 \qquad (2a \text{ y } 2b \text{ ambos pares en } \mathbb{Z}).$$

Si α es irracional, sea $\alpha = a+b\sqrt{d}$ con a y b en $\mathbb{Z}$, α entero, entonces α satisface una ecuación

$$x^2+bx+c=0, \quad \text{donde } b \text{ y } c \text{ están en } \mathbb{Z}.$$

Además $\quad x^2+bx+c = (x-\alpha)(x-\bar{\alpha})$

por lo que $\quad b = -(\alpha+\bar{\alpha}) = -2a$

y $$c = \alpha\bar{\alpha} = a^2 - b^2 d .$$

Como $b = -2a$ está en $\mathbb{Z}$ se tiene que a está en $\mathbb{Z}$ o $a = a'/2$ donde a' está en $\mathbb{Z}$., de cualquier manera $a = a'/2$ con a' en $\mathbb{Z}$.

También

$c = a^2 - b^2 d$ está en $\mathbb{Z}$ o sea

$(a'/2)^2 - b^2 d$ está en $\mathbb{Z}$ es decir

$a'^2/4 - b^2 d$ está en $\mathbb{Z}$,

como d está en $\mathbb{Z}$ se debe tener que

$$a'^2/4 - b^2 d = n, \qquad n \text{ en } \mathbb{Z}$$

de aquí que $a'^2 - 4b^2 d = 4n$ está en $\mathbb{Z}$.,

y por tanto $4b^2$ está en $\mathbb{Z}$ de donde $b = b'/2$ con b' en $\mathbb{Z}$. Sea

$$c = a^2 - b^2 d = (a'^2 - b'^2 d)/4 = n, \quad n \text{ en } \mathbb{Z}$$

por lo tanto $a'^2 - b'^2 d = 4n$ ⊛.

Se sabe que, si k es par, entonces $k^2 \equiv 0 \pmod 4$ y si k es impar, entonces $k^2 \equiv 1 \pmod 4$.

Si $d \equiv 1 \pmod 4$, entonces en la ecuación ⊛ resulta que

$$a'^2 - b'^2 \equiv 0 \pmod 4$$

de donde $$a'^2 \equiv b'^2 \pmod 4$$

por lo que $$a' \equiv b' \pmod 2$$

y así que $\alpha = (a' + b'\sqrt{d})/2$

donde a' y b' tienen la misma paridad.

Si $d \not\equiv 1 \pmod 4$, entonces en la ecuación (*) resulta que

$$a'^2 \equiv b'^2 d \pmod 4,$$

se examinan los casos:

Si $d \equiv 0 \pmod 4$, entonces $a'^2 \equiv 0 \pmod 4$ y así es que a' es par por lo que $a = a'/2$ está en $\mathbb{Z}$.

Como

$(a^2 - b^2 d)$ está en $\mathbb{Z}$

entonces $b^2 d$ está en $\mathbb{Z}$

por lo que b^2 está en $\mathbb{Z}$

y por consiguiente b está en $\mathbb{Z}$.

Así $\alpha = a + b\sqrt{d}$ con a y b en $\mathbb{Z}$.

En el caso $d \equiv 2, 3 \pmod 4$ se tiene que

$$b'^2 \equiv 0 \pmod 4 \text{ y } a'^2 \equiv 0 \pmod 4$$

de donde $a = a'/2$ y $b = b'/2$ son enteros racionales y en consecuencia $\alpha = a + b\sqrt{d}$, con a y b en $\mathbb{Z}$.

COROLARIO 2.3. Si $d \equiv 1 \pmod 4$, un número de $\mathbb{Q}(\sqrt{d})$ es entero si y sólo si puede ser expresado en la forma

$$a + b[(1 + \sqrt{d})/2]$$

con a y b en $\mathbb{Z}$.

Dem. Si a y b están en $\mathbb{Z}$, entonces

$$a+b[(1+\sqrt{d})/2] = [(2a+b)+b\sqrt{d}]/2$$

donde $2a+b \equiv b \pmod 2$ y así $(2a+b)$ y b tienen la misma paridad.

Del mismo modo, si a y b están en $\mathbb{Z}$, con la misma paridad, entonces

$$(a+b\sqrt{d})/2 = (a-b)/2 + b[(1+\sqrt{d})/2],$$

donde $(a-b)/2$ y b están en $\mathbb{Z}$, dado que $a \equiv b \pmod 2$.

TEO. 2.4. Si α y β son enteros en $\mathbb{Q}(\sqrt{d})$, entonces $\alpha+\beta$, $\alpha-\beta$ y $\alpha\beta$ son enteros en $\mathbb{Q}(\sqrt{d})$.

Dem. Probaremos el teorema para ambos casos $d \not\equiv 1 \pmod 4$ y $d \equiv 1 \pmod 4$. Sea

$$\omega = \begin{cases} \sqrt{d} & \text{si } d \not\equiv 1 \pmod 4, \\ (1+\sqrt{d})/2 & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Sea γ un número de $\mathbb{Q}(\sqrt{d})$, por el TEO. 2.2. y el COROLARIO 2.3. una condición necesaria y suficiente para que γ sea entero es que γ pueda ser expresado en la forma

Δ $\qquad \gamma = (\text{entero racional}) + (\text{entero racional})\,\omega.$

Si α y β son enteros en $\mathbb{Q}(\sqrt{d})$, entonces

$$\alpha = a+b\omega \quad \text{y} \quad \beta = c+e\omega$$

con a, b, c y e en $\mathbb{Z}$.

Así $\alpha+\beta=(a+b\omega)+(c+e\omega)$

$=(a+c)+(b+e)\omega$

$\alpha-\beta=(a+b\omega)-(c+e\omega)$

$=(a-c)+(b-e)\omega$

estando ambos en la forma Δ y por lo cual son enteros en $\mathbb{Q}(\sqrt{d})$. Escribamos

$$\omega^2=s\omega+t, \qquad \text{con } s \text{ y } t \text{ en } \mathbb{Z},$$

de donde, si $d\not\equiv 1 \pmod 4$, entonces $s=0$ y $t=d$, y si $d\equiv 1 \pmod 4$, entonces $s=1$ y $t=(d-1)/4$ con t entero racional dado que $d\equiv 1 \pmod 4$.

Así $\alpha\beta=(a+b\omega)(c+e\omega)$

$=ac+ae\omega+bc\omega+be\omega^2$

$=ac+(ae+bc)\omega+be(s\omega+t)$

$=(ac+bet)+(ae+bc+bes)\omega,$

al cual está expresado en la forma Δ, y por lo tanto $\alpha\beta$ es entero en $\mathbb{Q}(\sqrt{d})$.

Def. 2.5. Un Anillo R es un conjunto con dos operaciones binarias (adición y multiplicación) tales que:

1) R es un grupo abeliano bajo la adición.

2) La multiplicación es asociativa $(XY)Z=X(YZ)$

y distributiva respecto a la adición

$$X(Y+Z) = XY + XZ \,, \quad (Y+Z)X = YX + ZX .$$

3) Existe un único "1" en R tal que

$$X \cdot 1 = 1 \cdot X = X, \qquad \text{para todo } X \text{ en } R .$$

Si R cumple con las propiedades 1) al 4), entonces R es un anillo conmutativo con 1.

Denotaremos con $R(\sqrt{d})$ al conjunto de enteros de $\mathbb{Q}(\sqrt{d})$.

TEO. 2.6. $R(\sqrt{d})$ es un anillo conmutativo con 1.

Def. 2.7. Si R es un anillo conmutativo, entonces $a \neq 0$ en R se dice que es un divisor de cero si existe un $b \neq 0$ en R tal que $ab = 0$.

Def. 2.8. Un anillo conmutativo R es un Dominio entero si no tiene divisores de cero. Es decir si $ab = 0$ para algunos a y b en R, entonces al menos uno de los dos a o b es cero.

TEO. 2.9. $R(\sqrt{d})$ es un dominio entero.

Def. 2.10. Un anillo R puede sumergirse en un anillo R' si hay un Isomorfismo de R en R'. (Si R y R' tienen elementos unidad 1 y 1' exigimos, además que este isomorfismo lleve 1 en 1'). A R' le llamaremos sobre anillo o extensión de R si R puede sumergirse en R'.

TEO. 2.11. $\mathbb{Q}(\sqrt{d})$ es el campo de cocientes de $R(\sqrt{d})$.

TEO. 2.12. Si α es entero, entonces $N(\alpha)$ es entero racional.

Dem: Si α es entero, entonces $\bar{\alpha}$ es entero. (Esto se sigue de Def. 2.1 o TEO. 2.2.)
Así por el TEO. 2.4.,

$$N(\alpha) = \alpha\bar{\alpha} \quad \text{es entero.}$$

Pero $N(\alpha)$ es también racional, y por lo que $N(\alpha)$ es un entero racional.

§.3. DIVISIBILIDAD y FACTORIZACION EN PRIMOS

En esta sección estudiaremos la teoría de la divisibilidad del anillo de enteros $R(\sqrt{d})$.

Def. 3.1. Si α y β están en $R(\sqrt{d})$, con $\alpha \neq 0$, se dice que α divide a β y escribimos $\alpha \mid \beta$ si existe γ en $R(\sqrt{d})$ tal que $\beta = \alpha\gamma$ (en otras palabras $\alpha \mid \beta$ si β/α es entero).

TEO. 3.2. Si $\alpha \mid \beta$, entonces $\bar{\alpha} \mid \bar{\beta}$.
Si $\alpha \mid \beta$ y $\alpha \mid \gamma$, entonces para cualesquiera δ y δ' enteros de $R(\sqrt{d})$ $\alpha \mid (\beta\delta + \gamma\delta')$. [Casos particulares $\alpha \mid (\beta+\gamma)$, $\alpha \mid (\beta-\gamma)$ y $\alpha \mid \beta\delta$].
Si $\alpha \mid \beta$ y $\beta \mid \gamma$, entonces $\alpha \mid \gamma$.

Demo Si $\alpha \mid \beta$, entonces existe θ en $R(\sqrt{d})$ tal que $\beta = \alpha\theta$ de aquí que $\bar{\beta} = \bar{\alpha}\bar{\theta}$ y por definición $\bar{\alpha} \mid \bar{\beta}$.
Si $\alpha \mid \beta$ y $\alpha \mid \gamma$, entonces existen θ y η en $R(\sqrt{d})$ tal que

$$\beta = \alpha\theta \quad \text{y} \quad \gamma = \alpha\eta$$

así que

$$\beta\delta + \gamma\delta' = \alpha\theta\delta + \alpha\eta\delta' = \alpha(\theta\delta + \eta\delta').$$

Por lo tanto por el TEO. 2.4. y Def. 3.1

$$\alpha \mid (\beta\delta + \gamma\delta').$$

Si $\alpha \mid \beta$ y $\beta \mid \gamma$, entonces existen θ y η

en $R(\sqrt{d})$ tal que

$$\beta = \alpha\theta \quad y \quad \gamma = \beta\eta$$

de aquí que

$$\gamma = \beta\eta = (\alpha\theta)\eta = \alpha(\theta\eta),$$

por lo que $\alpha \mid \gamma$.

Def. 3.3. Un entero ε en $R(\sqrt{d})$ es llamado una <u>Unidad</u> si $\varepsilon \mid 1$. En particular 1 y -1 son unidades en $R(\sqrt{d})$.

TEO. 3.4. Si ε_1 y ε_2 son unidades en $R(\sqrt{d})$, entonces $\bar{\varepsilon}_1$, $\varepsilon_1\varepsilon_2$ y $\varepsilon_1/\varepsilon_2$ son unidades en $R(\sqrt{d})$.
Un entero ε en $R(\sqrt{d})$ es unidad si y sólo si $N(\varepsilon) = \pm 1$.

Demo Dado que ε_1 y ε_2 son unidades, existen enteros δ_1 y δ_2 en $R(\sqrt{d})$ tal que $\varepsilon_1\delta_1 = \varepsilon_2\delta_2 = 1$.
Así tenemos

$$\bar{\varepsilon}_1\bar{\delta}_1 = \overline{(\varepsilon_1\delta_1)} = \bar{1} = 1,$$

$$(\varepsilon_1\varepsilon_2)(\delta_1\delta_2) = (\varepsilon_1\delta_1)(\varepsilon_2\delta_2) = 1,$$

de donde $\bar{\varepsilon}_1$ y $\varepsilon_1\varepsilon_2$ son unidades.

Ahora bien

$$\varepsilon_1/\varepsilon_2 = \varepsilon_1\delta_2/\varepsilon_2\delta_2 = \varepsilon_1\delta_2$$

es un entero y $(\varepsilon_1/\varepsilon_2)(\varepsilon_2\delta_1) = 1$ con $\varepsilon_2\delta_1$ entero.
Así que $\varepsilon_1/\varepsilon_2$ es también unidad.

i) Si $\varepsilon \mid 1$, entonces $\varepsilon\delta = 1$ y luego así

$N(\epsilon)\,N(\delta) = 1$ por lo que $N(\epsilon) = \pm 1$.

ii) Si $\eta\bar{\eta} = N(\eta) = \pm 1$, entonces $\eta \mid 1$.

Denotemos $\sqrt{-1} = i$.

TEO. 3.5. Si $d<0$, $d \neq -1$ y $d \neq -3$, entonces
$R(\sqrt{d})$ tiene exáctamente dos unidades ± 1.
$R(i)$ tiene exáctamente cuatro unidades ± 1 y $\pm i$.
$R(\sqrt{-3})$ tiene exáctamente seis unidades ± 1, $(\pm 1+\sqrt{-3})/2$ y $(\pm 1-\sqrt{-3})/2$.

$\Delta\Delta$ Si $d>0$, entonces $R(\sqrt{d})$ tiene una infinidad de unidades.

Dem: Tomando nota del TEO. 3.4. se busca todos los enteros α en $R(\sqrt{d})$ tales que $N(\alpha) = \pm 1$.
De acuerdo con el TEO. 2.2. α puede expresarse en la forma

$$a+b\sqrt{d} \qquad \text{si } d \not\equiv 1 \pmod 4$$

o

$$(a+b\sqrt{d})/2 \qquad \text{si } d \equiv 1 \pmod 4.$$

Así es que $N(\alpha) = a^2 - b^2 d$ o $N(\alpha) = (a^2 - b^2 d)/4$.

Supóngase que $d<0$ y $d \not\equiv 1 \pmod 4$. Si α es unidad, entonces $N(\alpha) = \pm 1$ y de hecho $N(\alpha) = 1$ dado que $N(\alpha) \geq 0$ (TEO. 1.15.). Sea

$$N(\alpha) = a^2 - b^2 d = a^2 + b^2(-d).$$

Para $d \leq -2$ $(-d \geq 2)$, $N(\alpha) \geq a^2 + 2b^2$ y si $b \neq 0$ $(b^2 \geq 1)$, por lo que $N(\alpha) \geq a^2 + 2 \cdot 1 \geq 2$

con lo que α no es unidad. Así, si α es unidad y $d \leq -2$, entonces $b=0$ y $N(\alpha)=a^2=1$.
De donde $a=\pm 1$ y $\alpha=\pm 1$.

Supóngase que $d<0$ y $d \equiv 1 \pmod 4$. $N(\alpha) \geq 0$ y por tanto $N(\alpha)=1$. Entonces α es unidad si y sólo si $N(\alpha)=1$. Sea

$$a^2+b^2(-d)=4.$$

Para $d \leq -7$ $(-d \geq 7)$ y $b \neq 0$,

$$a^2+b^2(-d) \geq a^2+7b^2 \geq a^2+7 \cdot 1 \geq 7 > 4,$$

y por lo tanto α unidad implica que $b=0$, teniéndose así que $N(\alpha)=a^2=4$. De donde $a=\pm 2$ y $\alpha=\pm 1$.

Las unidades de $R(i)$ son

$$\varepsilon = i^s \qquad (s=0,1,2,3).$$

Ya que las únicas soluciones en $\mathbb{Z}$ de

$$a^2+b^2=1 \quad \text{son}$$

$$a=\pm 1 \text{ y } b=0 \quad \text{o} \quad a=0 \text{ y } b=\pm 1$$

y así que las unidades son ± 1 y $\pm i$.

Para $d=-3$, si α es unidad, entonces

$$a^2+3b^2=4.$$

Si $|b| \geq 2$, entonces $a^2+3b^2 \geq 12$ y así los valores posibles para b son $b=\pm 1, 0$.
Si $b=0$, entonces $a=\pm 2$ y $\alpha=\pm 1$.

Si $b=1$, entonces $a=\pm 1$ y $\alpha=(\pm 1+\sqrt{-3})/2$.

Si $b=-1$, entonces $a=\pm 1$ y $\alpha=(\pm 1-\sqrt{-3})/2$.

Procedamos a la demostración de $\Delta\Delta$, pero dada la complejidad ésto requiere de un análisis con ciertos resultados que nos ayudarán a resolver al problema.

Lema A. Sea θ irracional y $q>1$ entero racional positivo. Entonces existen x y y en $\mathbb{Z}$ tal que si $L=x-y\theta$,

$$|L|<1/q, \qquad 0<y\leq q. \tag{I}$$

Demo Sea y que toma los valores $0,1,\cdots,q$ y sea $x=[y\theta]$ tal que $0\leq L<1$.

Entonces los $q+1$ valores para L están en los q semi-intervalos abiertos

$$[r/q,\ r+1/q), \qquad r=0,1,\cdots,q-1.$$

Por lo tanto dos de los valores correspondientes a L a saber (x_1,y_1), (x_2,y_2), donde $y_1\neq y_2$ y digamos $y_1>y_2$, están en el mismo semiintervalo y así es que

$$|(x_1-x_2)-(y_1-y_2)\theta|<1/q.$$

Escribamos $x=x_1-x_2$, $y=y_1-y_2$ y sustituyamos en (I) de donde

$$|x-y\theta|<1/y,$$

de aquí que, hay entonces una infinidad de soluciones enteras para la desigualdad.

Lema B. Sea d entero racional positivo al cual no es cuadrado perfecto, existen una infinidad de parejas de enteros racionales X y Y los cuales satisfacen la desigualdad

$$|X^2 - Y^2 d| < 1 + 2\sqrt{d}.$$

Demo. Sea $\theta = \sqrt{d}$ en (I) y así es que los enteros racionales X y Y existen tal que

$$|X - Y\sqrt{d}| < 1/|Y|,$$

ésto por el Lema A. Entonces

$$|X + Y\sqrt{d}| = |X - Y\sqrt{d} + 2Y\sqrt{d}| < 1/|Y| + 2|Y|\sqrt{d},$$

de donde se tiene que

$$|X^2 - Y^2 d| = |X - Y\sqrt{d}|\,|X + Y\sqrt{d}| = 1/Y^2 + 2\sqrt{d} < 1 + 2\sqrt{d}.$$

TEO. 3. C. Sea d un entero racional positivo al cual no es cuadrado perfecto, existe al menos un par de enteros racionales X y Y los cuales satisfacen la ecuación

$$X^2 - dY^2 = 1 \qquad (II)$$

Demo. Se trata de probar que existe un entero racional tal que $|k| < 1 + 2\sqrt{d}$ y $k = X^2 - dY^2$ tiene una infinidad de soluciones enteras.
Supóngase que hay dos digamos X_1, Y_1 y X_2, Y_2 tal que

$$X_1 \equiv X_2,\ Y_1 \equiv Y_2 \pmod{|k|}, \quad (X_2, Y_2) \neq (-X_1, -Y_1) \qquad (III)$$

Por lo tanto, podamos suponer que

$$X_1^2 - dY_1^2 = X_2^2 - dY_2^2 = k,$$

donde X_1, Y_1, X_2, y Y_2 satisfacen la condición (III).

Ahora tenemos que

$$(X_1 - Y_1\sqrt{d})(X_2 + Y_2\sqrt{d}) = X_1X_2 - Y_1Y_2d + (X_1Y_2 - X_2Y_1)\sqrt{d}.$$

Por (I) y (III) tenemos

$$X_1X_2 - Y_1Y_2d \equiv X_1^2 - Y_1^2d \equiv 0 \pmod{|k|}$$

y

$$X_1Y_2 - X_2Y_1 \equiv X_1Y_1 - X_1Y_1 \equiv 0 \pmod{|k|}.$$

Por lo que $X_1X_2 - Y_1Y_2d = k\mu$

y $X_1Y_2 - X_2Y_1 = k\nu$,

donde μ y ν son enteros racionales.

Así que $(X_1 - Y_1\sqrt{d})(X_2 + Y_2\sqrt{d}) = k(\mu + \nu\sqrt{d})$

y

$$(X_1 + Y_1\sqrt{d})(X_2 - Y_2\sqrt{d}) = k(\mu - \nu\sqrt{d}).$$

Multiplicando miembro a miembro, se tiene que

$$(X_1^2 - Y_1^2d)(X_2^2 - Y_2^2d) = k^2 = k^2(\mu^2 - \nu^2d).$$

De donde tenemos que

$$\mu^2 - \nu^2d = 1.$$

Aquí $\nu \neq 0$. Ya que si $\nu = 0$, $X_1Y_2 = X_2Y_1$ y $\mu = \pm 1$

y $(X_1 - Y_1\sqrt{d})(X_2 + Y_2\sqrt{d})(X_2 - Y_2\sqrt{d}) = \pm k(X_2 - Y_2\sqrt{d})$.

Dividiendo entre k ambos miembros se tiene

$$(X_1 - Y_1\sqrt{d}) = \pm (X_2 - Y_2\sqrt{d}),$$

lo cual implica que $X_1 = \pm X_2$ y $Y_1 = \pm Y_2$. Pero nosotros podamos tomar $|X_1| \neq |X_2|$.

La ecuación (II) es llamada ecuación de Pell.

Sean d y k enteros racionales. Si $X=u$ y $Y=v$ son enteros racionales los cuales satisfacen la ecuación diofantina

$$X^2 - Y^2 d = k, \qquad \text{(IV)}$$

decimos, que el número

$$u + v\sqrt{d}$$

es una solución de (IV).

Las dos soluciones $u+v\sqrt{d}$ y $u'+v'\sqrt{d}$ son iguales si $u=u'$ y $v=v'$. La primera solución es mayor que la segunda si $u+v\sqrt{d} > u'+v'\sqrt{d}$.

Consideremos todas las soluciones $X+Y\sqrt{d}$ de la ecuación (II) con X, Y positivos. Entre estas existe una solución mínima $X_1+Y_1\sqrt{d}$, en la cual X_1 y Y_1 tienen sus mínimos valores positivos.

El número $X_1+Y_1\sqrt{d}$ es llamada solución fundamental de la ecuación (II).

Complemento del TEO. 3. C.

TEO. 3. C'. Si d es un número natural al cual no es un cuadrado perfecto, la ecuación (II) tiene una infinidad de soluciones $X+Y\sqrt{d}$.

Todas las soluciones con X y Y positivos se obtienen por la formula

$$X_n + Y_n\sqrt{d} = (X_1 + Y_1\sqrt{d})^n, \qquad (V)$$

donde $X_1+Y_1\sqrt{d}$ es la solución fundamental de (II), con $n \in \mathbb{N}$, y donde

$$X_n = X_1^n + \sum_{k=1} \binom{n}{2k} X_1^{n-2k} Y_1^{2k} d^k,$$

y

$$Y_n = \sum_{k=1} \binom{n}{2k-1} X_1^{n-2k+1} Y_1^{2k-1} d^{k-1}.$$

Dem. Claramente se sigue de (V) que

$$X_n - Y_n\sqrt{d} = (X_1 - Y_1\sqrt{d})^n. \qquad (VI)$$

dado que el conjugado de un producto es el producto de los conjugados. Ahora bien

$$X_n^2 - Y_n^2 d = (X_n + Y_n\sqrt{d})(X_n - Y_n\sqrt{d}) = (X_1 + Y_1\sqrt{d})^n (X_1 - Y_1\sqrt{d})^n$$
$$= (X_1^2 - Y_1^2 d)^n = 1,$$

de donde $X_n + Y_n\sqrt{d}$ es solución de (II).

Supóngase que $u + v\sqrt{d}$ es una solución no dada por (V). Entonces para algún $n \in \mathbb{N}$ se tiene que

$$(X_1 + Y_1\sqrt{d})^n < u + v\sqrt{d} < (X_1 + Y_1\sqrt{d})^{n+1}$$

y así

$$X_n + Y_n\sqrt{d} < u + v\sqrt{d} < (X_n + Y_n\sqrt{d})(X_1 + Y_1\sqrt{d}).$$

Entonces $1 < (u+v\sqrt{d})(x_n - y_n\sqrt{d}) < x_1 + y_1\sqrt{d}$. (VII)

Escribamos $(u+v\sqrt{d})(x_n - y_n\sqrt{d}) = x + y\sqrt{d}$,

donde $x = ux_n - vy_n d$ y $y = vx_n - uy_n$, nosotros podemos también tener que

$$(u - v\sqrt{d})(x_n + y_n\sqrt{d}) = x - y\sqrt{d}$$

y así $$1 = (u^2 - v^2 d)(x_n^2 - y_n^2 d) = x^2 - y^2 d.$$

Por lo que al número $x + y\sqrt{d}$ es solución de (II). Además, por (VIII) tenemos que $x + y\sqrt{d} > 1$, y, por otro lado,

$$0 < 1/x + y\sqrt{d} = x - y\sqrt{d} < 1.$$

Por lo tanto, se sigue de (VII) que

$$x + y\sqrt{d} < x_1 + y_1\sqrt{d}.$$

Pero ésto es imposible, dado que $x_1 + y_1\sqrt{d}$ es la solución fundamental.

Hablemos un poco de la ecuación

$$x^2 - y^2 d = -1 \qquad \text{☹}$$

Una condición necesaria para que ☹ tenga solución es que d no sea divisible por 4 ó cualquier primo $\equiv 3 \pmod 4$.

Es facil checar que ☹ tiene solución cuando $d = p$ primo $\equiv 1 \pmod 4$.

El cual lo presentamos como

TEO. 3. D. Si $P \equiv 1 \pmod 4$, entonces la ecuación diofantina

$$\xi^2 - P\eta^2 = -1,$$

tiene soluciones enteras ξ y η.

Demo Sea $X_1 + Y_1\sqrt{P}$ la solución mínima de la ecuación

$$X^2 - PY^2 = 1.$$

Entonces $X_1^2 - 1 = PY_1^2$. Δ

Aquí X_1 no puede ser par, para este caso debemos tener que $-1 \equiv P \pmod 4$.

Si X es impar, entonces $(X_1 - 1, X_1 + 1) = 2$.
Por lo tanto se sigue de Δ que

$$X_1 \pm 1 = 2\xi^2, \quad X_1 \mp 1 = 2P\eta^2,$$

donde ξ y η son números naturales y $Y_1 = 2\xi\eta$.

Por eliminación de X_1 tenemos que

$$\xi^2 - P\eta^2 = \pm 1.$$

Dado que $\eta < Y_1$, no podemos tener el signo "+". Y así el signo "−" es el que se toma.

Hablemos de la factorización de enteros no unidad en $R(\sqrt{d})$.

Notemos primero que si α está en $R(\sqrt{d})$, y si $N(\alpha) = 0$, entonces $\alpha = 0$ y si $N(\alpha) = 1$, entonces α es unidad.

De donde α en $R(\sqrt{d})$ no es cero, no unidad si y sólo si $N(\alpha) \geq 2$.

Def. 3.6. Un entero π en $R(\sqrt{d})$, no unidad es llamado Primo en $R(\sqrt{d})$ si para toda descomposición de π en producto de dos enteros $\pi = \alpha\beta$, se tiene que uno de ellos es unidad.

Def. 3.7. Un entero no cero, no unidad y no primo es llamado Compuesto.

TEO. 3.8. Si α está en $R(\sqrt{d})$ y $N(\alpha)$ es primo racional, entonces α es primo en $R(\sqrt{d})$.

Dem. Supongamos que $N(\alpha)$ es primo racional. Sea $\alpha = \beta\gamma$ donde β y γ están en $R(\sqrt{d})$,

$$N(\alpha) = N(\beta)\,N(\gamma),$$

donde $N(\beta)$ y $N(\gamma)$ son enteros racionales, pero por definición de primo racional $N(\beta)$ o $N(\gamma)$ es una unidad racional. Las unidades racionales son ± 1 y entonces $N(\beta) = \pm 1$ o $N(\gamma) = \pm 1$.

Por tanto β o γ es unidad. Y entonces α es primo.

Def. 3.9. Si α y β son enteros ninguno de los dos cero y tales que $\alpha = \beta\varepsilon$, donde ε es unidad, entonces α se dice que es un asociado de β.

En otras palabras, α es un asociado de β si y sólo si α/β es unidad.

Bajo esta definición cualquier α en $R(\sqrt{d})$ es un asociado de al mismo.

TEO. 3.10. Si α y β están en $R(\sqrt{d})$, entonces α es un asociado de β si y sólo si β es un asociado de α, es decir α y β son asociados.

Además α y β son asociados si y sólo si $\alpha \mid \beta$ y $\beta \mid \alpha$. Si α y β son asociados y $\gamma \mid \alpha$, entonces $\gamma \mid \beta$, y Si $\alpha \mid \delta$, entonces $\beta \mid \delta$.

Si α es primo, entonces todo asociado de α es primo. Si α es compuesto, entonces todo asociado de α es compuesto.

Dem: Si ε es unidad, entonces $1/\varepsilon$ es unidad.

Sea β asociado de α y sea $\alpha = \beta\varepsilon$, se tiene que $\beta = \alpha(1/\varepsilon)$, ε y $1/\varepsilon$ son unidades y enteros entonces $\alpha \mid \beta$ y $\beta \mid \alpha$ por definición de divisibilidad.

Por otro lado, si $\alpha \mid \beta$ y $\beta \mid \alpha$, entonces existen ε y δ enteros tales que $\beta = \alpha\varepsilon$ y $\alpha = \beta\delta$ y por tanto se tiene que $\varepsilon\delta = (\beta/\alpha)(\alpha/\beta) = 1$ y de aquí que ε y δ son unidades, además α y β son asociados.

Si α y β son asociados y $\gamma \mid \alpha$, como $\alpha \mid \beta$ se tiene que $\gamma \mid \beta$.

Si α y β son asociados y $\alpha \mid \delta$, como $\beta \mid \alpha$ se tiene que $\beta \mid \delta$.

Supóngase que α y β son no cero, no unidad enteros asociados en $R(\sqrt{d})$. Entonces cada vez que α es primo o compuesto, lo mismo para con β.

Mostraremos que α y β son ambos primos o ambos compuestos.

Supongamos que α es primo y β es compuesto sea $\beta = \gamma\delta$ donde ni γ, ni δ son unidades. Además α y β son asociados entonces existe ε unidad tal que $\alpha = \beta\varepsilon$.

Luego entonces $\alpha = (\gamma\delta)\varepsilon = \gamma(\delta\varepsilon)$, como γ no es unidad y $(\delta\varepsilon)$ es un asociado de una no unidad, $(\delta\varepsilon)$ es no unidad. Entonces α se ha expresado como

producto de dos no unidades contradiciendo al hecho de que α es primo. Por lo que deducimos que α y β son ambos primos o ambos compuestos.

TEO. 3.11 Si $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_n$ son enteros no cero en $R(\sqrt{d})$ y $\alpha = \alpha_1\alpha_2\cdots\alpha_n$ con $n > \log_2(|N(\alpha)|)$ entonces por lo menos uno de los α_j, $1 \le j \le n$ es una unidad. De aquí que si α no es una unidad, entonces α se puede expresar como producto de un número finito de primos del anillo $R(\sqrt{d})$.

Dem: Supóngase que ninguno de los α_j $(1 \le j \le n)$ son unidades entonces $|N(\alpha)| \ge 2$ para toda j.

Entonces

$$|N(\alpha)| = |N(\alpha_1)N(\alpha_2)\cdots N(\alpha_n)|$$

$$= |N(\alpha_1)||N(\alpha_2)|\cdots|N(\alpha_n)|$$

$$\ge 2\cdot 2\cdots 2 = 2^n.$$

Así que $\log_2(|N(\alpha)|) \ge \log_2 2^n = n$, contradiciendo al hecho de

$$n > \log_2(|N(\alpha)|),$$

de donde por lo menos uno de los α_j es una unidad.

Supongamos que α es entero no cero, no unidad, en $R(\sqrt{d})$. Mostraremos que α puede expresarse como el producto de uno o más primos de $R(\sqrt{d})$, lo cual haremos por inducción sobre la norma de α.

Si α no es cero, no unidad, entonces $|N(\alpha)| \ge 2$.

Si $|N(\alpha)| = 2$, entonces α es primo.

Si $|N(\alpha)| = 3$, entonces α es primo.

Hipótesis de inducción.
Si $|N(\alpha)| < n$, entonces α es producto de primos.

Supongamos que $|N(\alpha)| = n$, donde si n es primo ya está.
Si no lo es, entonces $\alpha = \gamma\beta$, y así

$$N(\alpha) = N(\gamma)N(\beta), \quad |N(\gamma)| < n \text{ y } |N(\beta)| < n$$

por tanto $\alpha = (p_1 p_2 \cdots p_s)(q_1 q_2 \cdots q_r)$
de donde tenemos un número finito de primos para la descomposición de α en primos.

§.4. FACTORIZACION UNICA Y DOMINIOS EUCLIDIANOS

Para quitarnos trabajar con unidades y asociados durante el desarrollo de la factorización de enteros definiremos una relación de equivalencia de la siguiente manera.

Denotemos con $\mathcal{U}(\sqrt{d})$ al conjunto de las unidades de $R(\sqrt{d})$.

$$\alpha \sim \varepsilon\alpha \qquad \text{para cualquier } \varepsilon \text{ en } \mathcal{U}(\sqrt{d}).$$

Veamos que está bien definida:

(i) $\alpha \sim \alpha$ ya que 1 está en $\mathcal{U}(\sqrt{d})$.

(ii) Si $\alpha \sim \beta$, entonces $\beta \sim \alpha$.

Si $\alpha \sim \beta$, entonces $\alpha = \varepsilon\beta$ con ε en $\mathcal{U}(\sqrt{d})$ de aquí que $\beta = (1/\varepsilon)\alpha$ además $1/\varepsilon$ está en $\mathcal{U}(\sqrt{d})$, así por tanto $\beta \sim \alpha$.

(iii) Si $\alpha \sim \beta$ y $\beta \sim \gamma$, entonces $\alpha \sim \gamma$.

Si $\alpha \sim \beta$ y $\beta \sim \gamma$, entonces, $\alpha = \varepsilon\beta$ y $\beta = \varepsilon'\gamma$ con ε y ε' en $\mathcal{U}(\sqrt{d})$. Tenemos así que

$$\alpha = \varepsilon\beta = \varepsilon(\varepsilon'\gamma) = (\varepsilon\varepsilon')\gamma = \varepsilon''\gamma,$$

ε'' está en $\mathcal{U}(\sqrt{d})$ de donde $\alpha \sim \gamma$.

Sea $\bar{\alpha}$ la clase de equivalencia de α.

En las clases de equivalencia se define el producto $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$ definiendo con ésto un semigrupo multiplicativo con $\bar{1}$ como unidad.

Def. 4.1. El anillo $R(\sqrt{d})$ se dirá Dominio de Factorización Unica (DFU) si y sólo si posee la siguiente propiedad:

Para todo α en $R(\sqrt{d})$, no cero, no unidad tal que se tengan representaciones

$$\bar{\alpha} = \bar{\pi}_1 \bar{\pi}_2 \cdots \bar{\pi}_k$$

y

$$\bar{\alpha} = \bar{q}_1 \bar{q}_2 \cdots \bar{q}_l$$

donde los $\bar{\pi}_1, \bar{\pi}_2, \cdots, \bar{\pi}_k, \bar{q}_1, \bar{q}_2, \cdots, \bar{q}_l$ son primos no necesariamente distintos, entonces $l=k$ y los multiconjuntos

$$\{\bar{\pi}_1, \bar{\pi}_2, \cdots, \bar{\pi}_k\} \quad \text{y} \quad \{\bar{q}_1, \bar{q}_2, \cdots, \bar{q}_l\}$$

son iguales.

[Los multiconjuntos son aquellos conjuntos en los cuales es valida la repetición de elementos].

TEO. 4.2. $R(\sqrt{d})$ es DFU si y sólo si tiene la siguiente propiedad:

Si $\pi \mid \alpha\beta$, donde π es primo y α y β son enteros, entonces $\pi \mid \alpha$ o $\pi \mid \beta$.

Demo: Supongamos que $R(\sqrt{d})$ es DFU y π un primo que divide al producto $\alpha\beta$.

Supóngase que $\pi \nmid \alpha$. Sean

$$\alpha = \epsilon \pi_1 \pi_2 \cdots \pi_r$$

y

$$\beta = \epsilon' q_1 q_2 \cdots q_s,$$

expresiones donde los $\pi_1, \pi_2, \cdots, \pi_r, q_1, q_2, \cdots, q_s$ son primos y ϵ, ϵ' unidades. Como

$$\overline{\pi} \mid \overline{\alpha}\,\overline{\beta}$$

entonces

$$\overline{\alpha}\,\overline{\beta} = \overline{\pi}\,\overline{\gamma}$$

donde $\overline{\gamma} = \overline{\gamma}_1 \overline{\gamma}_2 \cdots \overline{\gamma}_t$ con $\gamma_1, \gamma_2, \cdots, \gamma_t$ primos. Así

$$\overline{\pi}_1 \overline{\pi}_2 \cdots \overline{\pi}_r \overline{q}_1 \overline{q}_2 \cdots \overline{q}_s = \overline{\pi}\,\overline{\gamma}_1 \overline{\gamma}_2 \cdots \overline{\gamma}_t$$

por ser $R(\sqrt{d})$ DFU se tiene que

$$\{\overline{\pi}_1, \overline{\pi}_2, \cdots, \overline{\pi}_r, \overline{q}_1, \overline{q}_2, \cdots, \overline{q}_s\} = \{\overline{\pi}, \overline{\gamma}_1, \overline{\gamma}_2, \cdots, \overline{\gamma}_t\}$$

y como $\overline{\pi} \nmid \overline{\alpha}$ tenemos que $\overline{\pi} \neq \overline{\pi}_i$ para toda $1 \leq i \leq r$. Por lo que $\overline{\pi} = \overline{q}_j$ para alguna $1 \leq j \leq s$ y así $\pi \mid \beta$.

Sea $\alpha = \epsilon \pi_1 \pi_2 \cdots \pi_r = \epsilon' q_1 q_2 \cdots q_s$ fijemos π_i con $1 \leq i \leq r$.

Entonces $\pi_i \mid \epsilon' q_1 q_2 \cdots q_s$ es decir $\overline{\pi}_i \mid \overline{q}_1 \overline{q}_2 \cdots \overline{q}_s$. Si $\overline{\pi}_i \mid \overline{q}_1$, entonces $\overline{\pi}_i = \overline{q}_1$. Si $\overline{\pi}_i \nmid \overline{q}_1$, entonces $\overline{\pi}_i \mid \overline{q}_2 \cdots \overline{q}_s$ y por inducción en el número de factores se tiene que $\pi_i \mid q_j$ para alguna $2 \leq j \leq s$ así que $\overline{\pi}_i = \overline{q}_j$.

Repitiendo éste procedimiento se ve que $r = s$ y

$$\{\overline{\pi}_1, \overline{\pi}_2, \cdots, \overline{\pi}_r\} = \{\overline{q}_1, \overline{q}_2, \cdots, \overline{q}_s\}.$$

Def. 4.3. Sea $R(\sqrt{d})$ DFU, α y β elementos de $R(\sqrt{d})$.

Sean

$$\bar{\alpha} = \bar{\pi}_1 \bar{\pi}_2 \cdots \bar{\pi}_r$$

y

$$\bar{\beta} = \bar{q}_1 \bar{q}_2 \cdots \bar{q}_s$$

sus descomposiciones en primos. Definimos al máximo común divisor de $\bar{\alpha}$ y $\bar{\beta}$ como el producto de los elementos del multiconjunto intersección.

Se denotará como $(\bar{\alpha}, \bar{\beta}) = \bar{g}$, donde $\bar{g}$ es el máximo común divisor.

Si $(\bar{\alpha}, \bar{\beta}) = \bar{1}$, entonces $\bar{\alpha}$ y $\bar{\beta}$ son primos relativos.

TEO. 4.4. Supóngase que $R(\sqrt{d})$ tiene la propiedad de factorización única.

Si α, β y γ están en $R(\sqrt{d})$, $(\bar{\alpha}, \bar{\beta}) = \bar{1}$ y $\alpha\beta = \gamma^n$, donde n es entero racional positivo, entonces existen δ y η en $R(\sqrt{d})$ tales que $\alpha = \delta^n$ y $\beta = \eta^n$.

Demo Sea $\gamma = \pi_1 \pi_2 \cdots \pi_k$,

$$\bar{\alpha}\bar{\beta} = \overline{\alpha\beta} = \bar{\gamma}^n = \bar{\pi}_1^n \bar{\pi}_2^n \cdots \bar{\pi}_k^n .$$

Si $\bar{\pi}_i \mid \bar{\alpha}\bar{\beta}$, entonces $\bar{\pi}_i \mid \bar{\alpha}$ o $\bar{\pi}_i \mid \bar{\beta}$

Digamos que $\bar{\pi}_i \mid \bar{\alpha}$, como $(\bar{\alpha}, \bar{\beta}) = \bar{1}$, entonces

$$\bar{\pi}_i^n \mid \bar{\alpha} \quad \text{y} \quad \bar{\pi}_i^n \nmid \bar{\beta}$$

Análogo para $\bar{\pi}_i \mid \bar{\beta}$. De donde

$$\bar{\alpha} = \bar{\pi}_{i_1}^n \bar{\pi}_{i_2}^n \cdots \bar{\pi}_{i_\ell}^n \quad \text{y} \quad \bar{\beta} = \bar{\pi}_{i_1}^n \bar{\pi}_{i_2}^n \cdots \bar{\pi}_{i_k}^n ,$$

por lo que $\bar{\alpha} = \bar{\delta}^n$ y $\bar{\beta} = \bar{\eta}^n$.

TEO. 4.5. Sean a y b elementos de $\mathbb{Z}$, $a \neq 0$ y $b \neq 0$, $(a,b) = g$. Si α en $R(\sqrt{d})$ es tal que $\alpha | a$ y $\alpha | b$, entonces $\alpha | g$. En particular, si $(a,b) = 1$, entonces los únicos divisores de a y b en $R(\sqrt{d})$ son unidades.

Dem: Si $(a,b) = g$, entonces existen enteros racionales r y s tal que $ar + bs = g$. Si $\alpha | a$ y $\alpha | b$, entonces $\alpha | ar + bs = g$.

Si $(a,b) = 1$, entonces $g = 1$ y como $\alpha | g$ se tiene que α es unidad.

Def. 4.6. Un campo cuadrático $\mathbb{Q}(\sqrt{d})$, es llamado <u>campo euclidiano</u> si tiene la siguiente propiedad:

Dados α y β elementos de $R(\sqrt{d})$, con $\beta \neq 0$ existen γ y δ en $R(\sqrt{d})$ tal que

$$\alpha = \gamma\beta + \delta, \qquad |N(\delta)| < |N(\beta)|.$$

Si $d < 0$, entonces podemos omitir las barras de valor absoluto dado que las normas son no negativas.

TEO. 4.7. Si $\mathbb{Q}(\sqrt{d})$ es campo euclidiano, α y β en $R(\sqrt{d})$ no ambos cero, entonces existe δ en $R(\sqrt{d})$ tal que:

1) $\delta | \alpha$ y $\delta | \beta$.

2) Si $\gamma | \alpha$ y $\gamma | \beta$, entonces $\gamma | \delta$.

Un entero δ' tiene las dos propiedades anteriores si y sólo si δ' es asociado de δ.

Además, si δ entero cumple con 1) y 2), entonces se puede expresar como combinación lineal de α y β, es decir existen θ y η en $R(\sqrt{d})$ tal que

3) $\delta = \alpha\theta + \beta\eta$.

Dem: Supongamos que $\beta \neq 0$, dado que $\alpha \neq 0$ y $\beta \neq 0$.

Por definición de campo euclidiano existen enteros γ_1 y β_1 tal que

$$\alpha = \gamma_1\beta + \beta_1, \qquad |N(\beta)| > |N(\beta_1)|.$$

Si $\beta_1 = 0$, hemos terminado.

Si $\beta_1 \neq 0$, entonces existen enteros γ_2 y β_2 tal que

$$\beta = \gamma_2\beta_1 + \beta_2, \qquad |N(\beta_1)| > |N(\beta_2)|.$$

Si $\beta_2 = 0$, hemos terminado.

Si $\beta_2 \neq 0$, entonces existen enteros γ_3 y β_3 tal que

$$\beta_1 = \gamma_3\beta_2 + \beta_3, \qquad |N(\beta_2)| > |N(\beta_3)|.$$

Nosotros continuamos éste proceso hasta llegar a $\beta_n = 0$.

De ésta manera obtenemos una sucesión de enteros $\beta, \beta_1, \beta_2, \ldots$ tal que $|N(\beta)| > |N(\beta_1)| > |N(\beta_2)| > \cdots$ y los números $|N(\beta_i)|$ son enteros racionales mayores o iguales a cero.

Una sucesión de enteros racionales no negativos decreciente es una sucesión finita. Como resultado existe un mínimo β_s en la sucesión a saber β_n.

Así tenemos una sucesión de ecuaciones

$$\alpha = \gamma_1\beta + \beta_1$$

$$\beta = \gamma_2 \beta_1 + \beta_2$$
$$\beta_1 = \gamma_3 \beta_2 + \beta_3$$
$$\vdots$$
$$\beta_{n-3} = \gamma_{n-1} \beta_{n-2} + \beta_{n-1}$$
$$\beta_{n-2} = \gamma_n \beta_{n-1} + 0.$$

El número β_{n-1} será el δ del teorema.

Por la última ecuación $\beta_{n-1} \mid \beta_{n-2}$, por la ecuación anterior a la última $\beta_{n-1} \mid \beta_{n-3}$, por la ecuación anterior a la penúltima $\beta_{n-1} \mid \beta_{n-4}$ y así sucesivamente. Llegando a la segunda de éstas ecuaciones con $\beta_{n-1} \mid \beta_2$ y $\beta_{n-1} \mid \beta_1$ de donde $\beta_{n-1} \mid \beta$ y teniendo finalmente de la primera ecuación que $\beta_{n-1} \mid \alpha$. Esta es la propiedad 1) de el teorema.

Otra vez

$$\beta_{n-1} = \beta_{n-3} - \gamma_{n-1} \beta_{n-2}.$$

y así

$$\beta_{n-1} = \beta_{n-3} - \gamma_{n-1} (\beta_{n-4} - \gamma_{n-2} \beta_{n-3})$$
$$= -\gamma_{n-1} \beta_{n-4} + (1 + \gamma_{n-1} \gamma_{n-2}) \beta_{n-4},$$

es una combinación lineal de β_{n-4} y β_{n-3}. Procediendo de esta manera llegaremos a expresar

$$\beta_{n-1} = \alpha\theta + \beta\eta$$

para algunos θ y η enteros. Por lo tanto cualquier divisor de α y β es también divisor de β_{n-1} y ésta es la propiedad 2) de el teorema.

Es claro que cualquier asociado de β_{n-1} cumple con las propiedades 1) y 2). Además, si δ' cumple con estas propiedades, entonces usando la propiedad 2)

para β_{n-1} y δ', $\beta_{n-1} | \delta'$ y $\delta' | \beta_{n-1}$. Por el TEO.3.10. δ' y β_{n-1} son asociados.

Si ε es unidad, entonces

$$\varepsilon \beta_{n-1} = \alpha(\varepsilon\theta) + \beta(\varepsilon\eta),$$

por lo que cualquier asociado de β_{n-1} puede ser expresado en la forma de la propiedad 3) de el teorema

De esta manera se ha mostrado que cualquier δ que cumpla con 1) y 2) también cumple con 3).

TEO.4.8. Un campo cuadrático euclidiano tiene la propiedad de factorización única.

Demo: Supóngase que $\mathbb{Q}(\sqrt{d})$ es euclidiano y $\pi | \alpha\beta$, donde π es primo, α y β enteros. Mostraremos que si $\pi \nmid \alpha$, entonces $\pi | \beta$; tomando nota del TEO.4.2.

Como $\pi \nmid \alpha$ ningún asociado de π divide a α.

Dado que π es primo cualquier divisor de π es, a su vez un asociado de π o una unidad. De estos dos hechos se muestra que un común divisor de α y π debe de ser una unidad. Cualquier unidad divide a 1, el número 1 cumple con las primeras dos propiedades de el número δ del TEO.4.7., así que $1 | \alpha$ y $1 | \beta$, y si $\gamma | \alpha$ y $\gamma | \pi$ (por lo que γ es unidad), entonces $\gamma | 1$.

Por el TEO.4.7., existen enteros θ y η tal que

$$\alpha\theta + \pi\eta = 1.$$

Luego tenemos que

$$\alpha\beta\theta + \pi\beta\eta = \beta,$$

de donde $\pi | \beta$.

Por lo tanto por el TEO. 4.2. $\mathbb{Q}(\sqrt{d})$ tiene la propiedad de factorización única.

TEO. 4.9. Si $d = -11, -7, -3, -2, -1, 2, 3, 5$, $\mathbb{Q}(\sqrt{d})$ es euclidiano.

Dem: Dividamos la demostración en dos casos a saber los $d \not\equiv 1 \pmod 4$ y los $d \equiv 1 \pmod 4$.

Supóngase que $d = -2, -1, 2, 3$. Sean α y β enteros tal que $\beta \neq 0$. Sea $\alpha/\beta = X + Y\sqrt{d}$, donde X y Y son racionales pero no necesariamente enteros racionales.

Dado que cualquier racional está entre dos enteros racionales consecutivos y en consecuencia escojamos los enteros racionales r y s que estén más próximos a X y Y, ésto es de manera que

$$0 \leq |X - r| \leq \tfrac{1}{2}, \qquad 0 \leq |Y - s| \leq \tfrac{1}{2}.$$

Sean $\gamma = r + s\sqrt{d}$, $\quad \delta = [(X - r) + (Y - s)\sqrt{d}]\,\beta$

así que $\alpha = \beta(X + Y\sqrt{d}) = \beta\gamma + \delta$.

Como r y s son enteros racionales, γ es entero y, δ es entero dado que $\delta = \alpha - \beta\gamma$. Ahora bien

$$|N(\delta)| = |N(\beta)|\,|N[(X - r) + (Y - s)\sqrt{d}]| = |N(\beta)|\,|(X - r)^2 - (Y - s)^2 d|$$

y de aquí $|(X - r)^2 - d(Y - s)^2| \leq |X - r|^2 + |-d|\,|Y - s|^2 \leq (1/2)^2 + 3(1/2)^2 = 1$

La igualdad puede ser posible sólo cuando

$$|X - r| = |Y - s| = 1/2 \quad \text{y} \quad d = 3,$$

y entonces $\quad |(X - r)^2 - d(Y - s)^2| = |1/4 - 3 \cdot 1/4| = 1/2 < 1$

por lo que $\quad |(X - r)^2 - d(Y - s)^2| < 1.$

Así $|N(\delta)| = |N(\beta)||(x-r)^2 - d(y-s)^2| < |N(\beta)| \cdot 1 = |N(\beta)|$.

Por lo que $\mathbb{Q}(\sqrt{d})$ es euclidiano.

Ahora supóngase que $d = -11, -7, -3, 5$. Sean, α y β enteros tal que $\beta \neq 0$. Sea $\alpha/\beta = x + y\sqrt{d}$, donde x y y son racionales.

El número $2y$ está entre enteros racionales consecutivos y existe un entero racional s tal que $|2y - s| \leq 1/2$ y así

$$|y - s/2| \leq 1/4.$$

Similarmente, existe un entero racional r tal que

$$|(x - s/2) - r| \leq 1/2.$$

Sean $$\gamma = r + s[(1+\sqrt{d})/2],$$

el cual es entero por el COROLARIO.2.3.

y $$\delta = [(x - r - s/2) + (y - s/2)\sqrt{d}]\,\beta.$$

Entonces $\alpha = \beta(x + y\sqrt{d}) = \beta\gamma + \delta$,

de donde δ es entero.

Ahora bien

$$|N(\delta)| = |N(\beta)|\,|(x - r - s/2)^2 - d(y - s/2)^2|$$

y de aquí $|(x - r - s/2)^2 - d(y - s/2)^2| \leq |x - r - s/2|^2 + |d|\,|y - s/2|^2$

$$\leq (1/2)^2 + 11(1/4)^2 < 1$$

Así que $|N(\delta)| < |N(\beta)|$

con lo que $\mathbb{Q}(\sqrt{d})$ es euclidiano.

Los tres teoremas siguientes sólo los anunciamos ya que sus demostraciones no están al alcance de esta tesis.

TEO. 4.10. $\mathbb{Q}(\sqrt{d})$ es euclidiano si y sólo si $d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

TEO. 4.11. Si $d < 0$, entonces $\mathbb{Q}(\sqrt{d})$ tiene la propiedad de factorización única si y sólo si $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

TEO. 4.12. Hay exáctamente 38 campos cuadráticos reales, $\mathbb{Q}(\sqrt{d})$, que tienen la propiedad de factorización única con $2 \leq d < 100$. Estos son

$d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$.

TEO. 4.13. Si $R(\sqrt{d})$ es DFU, entonces 2 no es primo en $R(\sqrt{d})$.

Dem: Como $2 \mid d(d-1)$, se tiene que

$$(d+\sqrt{d})(d-\sqrt{d}) = d^2 - d = d(d-1)$$

de donde $2 \mid (d+\sqrt{d})(d-\sqrt{d})$.

Pero en $R(\sqrt{d})$, $2 \nmid (d+\sqrt{d})$ y $2 \nmid (d-\sqrt{d})$, dado que ninguno de los números $(d/2 + \frac{1}{2}\sqrt{d})$ y $(d/2 - \frac{1}{2}\sqrt{d})$ están en $R(\sqrt{d})$. Así, 2 divide un producto de dos números en $R(\sqrt{d})$, pero 2 no divide a ninguno de los dos factores. Por el TEO. 4.2., Si $R(\sqrt{d})$ es DFU, entonces 2 no es primo.

TEO. 4.14. Si $d<0$, entonces $R(\sqrt{d})$ es DFU si y sólo si $d=-1$ o $d=-2$. (por lo que si $d<0$, $d \not\equiv 1 \pmod 4$, entonces $R(\sqrt{d})$ tiene la propiedad de factorización única si y sólo si $d=-1$ o $d=-2$). Si $d \equiv 1 \pmod 4$, entonces $R(\sqrt{d})$ nunca es DFU.

Demo Mostraremos que si $d \leq -3$ o $d \equiv 1 \pmod 4$, entonces 2 es primo en $R(\sqrt{d})$, y para ésto utilizaremos el TEO. 4.13.

Queremos mostrar que $R(i)$ y $R(\sqrt{-2})$ son dominios de factorización única. Cuando consideramos $d<0$, podemos restringir nuestra atención a los $d \leq -3$.

Supóngase que 2 no es primo en $R(\sqrt{d})$. Entonces existen α y β en $R(\sqrt{d})$ tal que

$$2 = \alpha\beta, \qquad |N(\alpha)|>1, \ |N(\beta)|>1.$$

Como $N(\alpha)N(\beta)=4$ y dado que $|N(\alpha)|$ y $|N(\beta)|$ son enteros racionales mayores que uno,

$$|N(\alpha)| = |N(\beta)| = 2.$$

De donde si 2 no es primo en $R(\sqrt{d})$, entonces existe un número

$$\alpha = a + b\sqrt{d}, \qquad (a \text{ y } b \text{ en } \mathbb{Z})$$

tal que $N(\alpha) = a^2 - b^2 d = \pm 2$ ⊙

Si $d \leq -3$ y $b \neq 0$, entonces

$$a^2 - db^2 = a^2 + (-d)b^2 \geq 0 + 3\cdot 1 > \pm 2,$$

mientras que si $b=0$, entonces

$$a^2 - b^2 d = a^2 \neq \pm 2, \qquad \text{con } a \text{ en } \mathbb{Z}.$$

Así que cuando $d \leq -3$, no existen números en $R(\sqrt{d})$ de norma ± 2 por lo que 2 es primo en $R(\sqrt{d})$. y por el TEO. 4.13., si $d \leq -3$, entonces $R(\sqrt{d})$ no es DFU.

Ahora supongamos que $d \equiv 1 \pmod 4$. Módulo 4 la ecuación $\odot$ se reduce a

$$a^2 - b^2 \equiv a^2 - b^2 d \equiv \pm 2 \equiv 2 \pmod 4.$$

Pero los cuadrados (mod 4) son 0 y 1 y por tanto $a^2 - b^2$ es congruente a $-1, 0, o\ 1 \pmod 4$. Así la congruencia

$$a^2 - b^2 \equiv 2 \pmod 4,$$

no tiene soluciones en los enteros racionales y de aquí que la ecuación $\odot$ es imposible.

Por lo tanto 2 es primo en $R(\sqrt{d})$ y por el TEO. 4.13. $R(\sqrt{d})$ no es DFU.

§.5. LOS PRIMOS EN $\mathbb{Z}[i]$

Ahora denotaremos con $\mathbb{Z}[i]$ al conjunto de los enteros gausianos.

$\mathbb{Z}[i]$ es DFU lo cual fué mostrado por Gauss y de ahí que a estos números se les da el nombre de gausianos.

TEO.5.1. Sea p primo racional positivo.
Si $p \equiv 3 \pmod 4$, entonces p es primo en $\mathbb{Z}[i]$.
Si $p = 2$ o $p \equiv 1 \pmod 4$, entonces p no es primo en $\mathbb{Z}[i]$, y existe un primo π en $\mathbb{Z}[i]$ tal que $N(\pi) = p$.
Si π es primo en $\mathbb{Z}[i]$, entonces π es un asociado de un primo racional $\equiv 3 \pmod 4$ o $N(\pi)$ es primo racional $\equiv 1 \pmod 4$ o $N(\pi) = 2$.

Dem: Sea $p \equiv 3 \pmod 4$. Supóngase que p no es primo en $\mathbb{Z}[i]$, existen α y β enteros no unidades tal que $p = \alpha\beta$.

Así que $$p^2 = N(p) = N(\alpha)\,N(\beta)$$

y dado que las normas son no negativas en $\mathbb{Z}[i]$

$$N(\alpha) > 1 \quad y \quad N(\beta) > 1$$

de donde $$N(\alpha) = N(\beta) = p .$$

Sea $\alpha = a + bi$ entero de $\mathbb{Z}[i]$, entonces

$$a^2+b^2 = N(\alpha) = p \qquad *$$

pero $a^2+b^2 \not\equiv 3 \pmod 4$ de aquí que * no es posible.

Si $p=2$, entonces $N(1+i)=2$ de donde $1+i$ es primo en $\mathbb{Z}[i]$.

Si $p \equiv 1 \pmod 4$, entonces existe un entero racional a tal que

$$a^2+1 \equiv 0 \pmod p$$

(Véase TEO. 2.11 del libro Teoría de los números de Niven y Zuckerman), así que existe un entero racional b tal que

$$a^2+1 = pb$$

o

$$(a+i)(a-i) = pb .$$

Como p es primo y $\mathbb{Z}[i]$ es DFU,

$$p \mid a+i \quad o \quad p \mid a-i .$$

Si $p \mid a+i$, entonces $a+i = p(c+di)$ es decir

$$a = pc \quad y \quad 1 = pd ,$$

pero $p>1$ de donde $1 = pd$ no es posible y de aquí que p no es primo en $\mathbb{Z}[i]$.

Por lo tanto existen enteros no unidades π_1 y π_2 tal que $p = \pi_1 \pi_2$, de tal manera que

$$N(\pi_1\pi_2) = N(\pi_1)N(\pi_2) = N(p) = p^2,$$

y como

$$N(\pi_1) > 1 \quad y \quad N(\pi_2) > 1$$

implica que

$$N(\pi_1) = p = N(\pi_2).,$$

de lo cual por el TEO.3.8., π_1 y π_2 son primos en $\mathbb{Z}[i]$.

Inversamente cualquier primo en $\mathbb{Z}[i]$ es un asociado de uno de los tres tipos dados anteriormente.

Sea π primo en $\mathbb{Z}[i]$, $N(\pi)$ es entero racional positivo mayor que uno por lo cual es igual a un producto de primos racionales, es decir

$$\pi\bar{\pi} = N(\pi) = p_1 p_2 \cdots p_n,$$

con los p_i $(1 \le i \le n)$ primos racionales. Como $\pi \mid \prod_{i=1}^{n} p_i$ y $\mathbb{Z}[i]$ es DFU se tiene que

$$\pi \mid p_j \qquad \text{para alguna } 1 \le j \le n.$$

Si $p_j \equiv 3 \pmod 4$, entonces p_j es primo en $\mathbb{Z}[i]$, y así p_j/π es una unidad y π es un asociado de p_j.

Si $p_j \not\equiv 3 \pmod 4$, entonces p_j no es primo y como se vio anteriormente $N(\pi) = p_j$.

TEO. 5.2. Sea n un entero racional positivo dado. La ecuación Diofantina

$$X^2 + Y^2 = n, \qquad \square$$

con X y Y no conocidos tiene una solución en enteros racionales si y sólo si n puede ser expresado en la forma $n = m^2 k$, donde m y k son enteros racionales y k no tiene divisores primos racionales positivos congruentes con $3 \pmod 4$.

(Así, por ejemplo 45 es la suma de dos cuadrados y 27 no lo es).

Demo: Supóngase que $n = m^2 k$ con m y k enteros racionales positivos tal que si P es un primo racional positivo divisor de k, entonces $P \not\equiv 3 \pmod 4$.

Si $k = 1$, entonces $n = m^2 + 0^2$. Si $k > 1$, entonces

$$k = P_1 P_2 \cdots P_r,$$

donde cada P_j es primo racional igual a 2 o congruente con $1 \pmod 4$.

Por lo que por el TEO. 5.1., existen primos $\pi_1, \pi_2, \cdots, \pi_r$ en $\mathbb{Z}[i]$ tal que

$$N(\pi_j) = P_j \quad \text{para toda } 1 \le j \le r.$$

Sea $a + bi = m \pi_1 \pi_2 \cdots \pi_r$,

$$\begin{aligned} a^2 + b^2 &= N(m)\, N(\pi_1)\, N(\pi_2) \cdots N(\pi_r) \\ &= m^2 P_1 P_2 \cdots P_r \\ &= m^2 k \\ &= n \end{aligned}$$

y así que □ tiene solución.

Inversamente, supóngase que existen enteros racionales a y b tal que

$$a^2+b^2=n \quad \text{o} \quad N(a+bi)=n.$$

Si $a+bi$ es unidad, entonces $n=1$, el cual puede ser expresado en la forma 1^2+0^2 que pide el teorema.

Si $a+bi$ no es unidad, entonces podemos factorizar $a+bi$ en un producto de primos, es decir

$$a+bi=\pi_1\pi_2\cdots\pi_r.$$

Por el TEO.5.1. podemos asumir que $\pi_1, \pi_2, \cdots, \pi_s$ son asociados de primos racionales $P_1, P_2, \cdots, P_s$ todos congruentes con 3 (mod 4), mientras que $\pi_{s+1}, \pi_{s+2}, \cdots, \pi_r$ tienen normas $P_{s+1}, P_{s+2}, \cdots, P_r$ los cuales son primos racionales cada uno igual a 2 o congruente con 1 (mod 4).

Sean $m=P_1P_2\cdots P_s$, $k=P_{s+1}P_{s+2}\cdots P_r$,

entonces vemos que

$$\begin{aligned} n &= N(a+bi) \\ &= N(\pi_1)N(\pi_2)\cdots N(\pi_s)N(\pi_{s+1})N(\pi_{s+2})\cdots N(\pi_r) \\ &= P_1^2P_2^2\cdots P_s^2P_{s+1}P_{s+2}\cdots P_r \\ &= m^2k. \end{aligned}$$

Además, los divisores primos racionales de k son 2 o los congruentes con 1 (mod 4) y así los primos racionales congruentes con 3 (mod 4) no dividen a k.

COROLARIO. 5.3. Sea P primo racional.
Si $P=2$ ó $P \equiv 1 \pmod 4$, entonces P puede ser expresado como la suma de dos cuadrados.
Si $P \equiv 3 \pmod 4$, entonces P no puede ser expresado como la suma de dos cuadrados.

BIBLIOGRAFIA

Apostol, T.M.: Introduction to Analitic Number Theory.

Birkhoff, G.: Modern Algebra (a survey of). 3a. edición. MacMilan Co.

Hardy, G.H. and Wright, E.M.: An Introduction to the theory of Numbers. Oxford University Press. Oxford. 1938.

Nagell, T. : Introduction to Number Theory. John Wiley & Sons, Inc. New York. 1951.

Niven y Zuckerman.: Introducción a la Teoría de los Números. Editorial Limosa.

Stark, H.M. : An Introduction to Number Theory. Markham Mathematics series. Chicago.

Vinogradov, I.M.: Elements of Number Theory. Dover Publications. 1954.